AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

32 Cedarwood Way, Apt C
Newport News, VA, 23608

UNDER SEAL

Case No. 4:20sw1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2) and 5(b)	Receipt, Distribution and Possession of Child Pornography

The application is based on these facts:

See affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

Lisa R. McKeel
Assistant United States Attorney

Applicant's signature

Heather Call, Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/9/2020

Judge's signature

City and state: Norfolk, VA

Douglas E. Miller
United States Magistrate Judge
Printed name and title

4:20sw1

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

Introduction and Agent Background

I, Heather Call, being duly sworn, hereby depose and state:

1. Your affiant, Heather Call, employed with the Newport News Police Department (NNPD) since June 2004, and more specifically with the Special Victims Unit since July 2011. This assignment has afforded me the opportunity to investigate and/or arrest and prosecute numerous individuals for crimes relating to the neglect and abuse of children in violation of the Virginia (VA) State Code. I have previously been involved in criminal investigations concerning violations of federal laws. Those investigations included, but are not limited to, child exploitation and child pornography. Since joining the NNPD your affiant has attended specialized training courses in child/adolescent interviewing, human trafficking, identifying and seizing electronic evidence, and computer forensic, recovery, and social site investigations.

2. I am currently assigned as a Master Police Detective with the Newport News Police Department, Criminal Investigations Division, Special Victims Unit, as well as a Task Force Officer (TFO) assigned to the Federal Bureau of Investigation, Norfolk Division Child Exploitation Task Force. I have participated in investigations involving sexual assaults, persons who collect and distribute child pornography, and distribution of materials relating to the sexual exploitation of children. I have received training from the FBI in the areas of sexual assaults and child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers.

3. In the course of my employment as a sworn law enforcement officer, I have

participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18, United States Code § 2251 *et. seq.* involving child exploitation offenses.

4. I was deputized as a Special Deputy United States Marshal on June 16, 2014. As a Special Deputy United States Marshal, your Affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

Location

5. This affidavit is made in support of an application for a warrant to search the entire premises located at **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608** (more precisely described in Attachment A).

6. This affidavit is based upon information that I have gained from my investigation, my training and experience, as well as information gained from conversations with other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities (more precisely described in Attachment B) of violations of Title 18, United States Code, § 2252A(a)(2) and (a)(5)(B) are located at the above address.

Pertinent Federal Criminal Statutes

7. This investigation concerns alleged violations of Title 18, United States Code, § 2252A(a)(2) and (a)(5)(B), relating to material involving the sexual exploitation of minors.

8. Title 18, United States Code, § 2252A(a)(2) makes it a federal criminal offense to knowingly receive or distribute any child pornography or materials that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

9. Title 18, United States Code, § 2252A(a)(5)(B) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

Definitions

10. The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

11. The terms "records," "documents," and "materials" include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

Graphic records or representations, photographs, pictures, images, and aural records or representations.

12. The terms "minor" and "sexually explicit conduct" are defined in Title 18, United States Code, Sections 2256(1) and (2). A "minor" is defined as "any person under the age of eighteen years." The term "sexually explicit conduct" means actual or simulated:

i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

ii. Bestiality;

iii. Masturbation;

iv. Sadistic or masochistic abuse; or

v. Lascivious exhibition of the genitals or pubic area of any person.

13. Universal Resource Locator (URL): A URL is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

14. Internet Protocol Address (IP Address): Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. There are two types of IP addresses, static and dynamic. A static address is permanent

and never changes, such as ones used in cable modems. The dynamic address changes almost every time the computer connects to the Internet.

15. The term "Internet Service Provider" (ISPs): This term refers to individuals who have an Internet account and an Internet-based electronic mail (e-mail) address, who must have a subscription, membership, or affiliation with an organization or commercial service that provides access to the Internet. A provider of Internet access and services is referred to as an Internet Service Provider or "ISP."

16. The term "Secure Hash Algorithm" (SHA-1) is one of a number of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard. SHA-1 is the original 160-bit hash function. It was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. The SHA-1 value is one form of an electronic fingerprint for a digital image.

17. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer

customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

18. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

19. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." 18 U.S.C. § 2711.

20. "Electronic Communications System" means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

21. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

22. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17).

Specifics of Search and Seizure of Computer System and Related Media

23. Your affiant, based on conversations with Computer Investigative Specialists, who have been trained in the seizure, examination and retrieval of data from personal computer systems and related media, knows that searching and seizing information from computer systems often

requires agents to seize all electronic storage devices to be searched later in a laboratory or other controlled environment.

24. Computer storage devices (like hard drives, diskettes, tapes, laser disks, and thumb or flash drives) can store enormous quantities of information. For instance, a single 200-gigabyte hard-drive may contain the electronic equivalent of hundreds of thousands of pages of double-spaced text. However, unlike the search of documentary files, computers store data in files that are often not easily reviewed. Additionally, a suspect may try to conceal criminal evidence by storing files in random order and/or with deceptive file names. This may require the examiner to examine all the stored data to determine which particular files are evidence or instrumentalities of the crime. This sorting process can take weeks or months, depending on the volume of data stored.

25. Searching computer systems for criminal evidence is a highly technical process, requiring specialized skills and a properly controlled environment. The vast array of computer hardware and software available requires even computer examiners to specialize in some systems and applications, so it is difficult to know before a search which computer investigative specialist is qualified to analyze the system and its data. In any event, the investigative specialist will use certified forensic tools and data search protocols that are designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (from external sources and/or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

26. An important step that is ordinarily part of an examiner's forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that

are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

Use of Computers with Child Pornography

27. Based upon my training and information officially supplied to me by other law enforcement officers, your affiant knows the following:

28. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. They have also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

29. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution and storage.

a. Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited in very similar ways to a photograph.

The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as methods that have been used in the past.

b. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of the computer has also changed that. A device known as a modem allows any computer to connect to another computer using telephone lines or other cable lines. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. These host computers are sometimes operated by commercial concerns, such as Microsoft and America Online, which allow subscribers to access their network services via connection through an Internet broadband provider or by dialing a local number and connecting via a telephone modem.

c. These service providers allow electronic mail ("e-mail") service between subscribers and between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web; hence, they are commonly described as Internet Service Providers (ISPs). Some of these systems offer their subscribers the ability to communicate publicly or privately with each other in real time using a mode of communication called instant messaging, or "IM." When logged into an IM service, users can search for other users based on the information that the other users have supplied, and they can send those users messages or initiate a chat session. Chat sessions can occur in multiple person groups, or in private one-on-one sessions. Most IM services also allow files to be transferred between users, including image files.

d. These communications structures are ideal for the child pornography collector. The open and anonymous communication allows users to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send text messages and graphic images to other trusted child pornography collectors. Moreover, the child pornography collectors can use standard Internet connections, such as those provided by business, universities, and government agencies, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornography collectors.

e. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred (via electronic mail, through file transfer protocols (FTPs), or via news group postings) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, and easy access to the Internet, the computer is a preferred method of distribution of child pornographic materials.

30. The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of five hundred (500) gigabytes are not uncommon. These drives can store hundreds of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

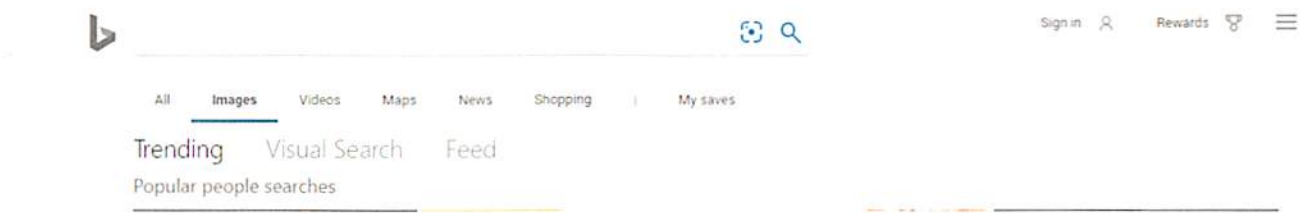
31. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for extended periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

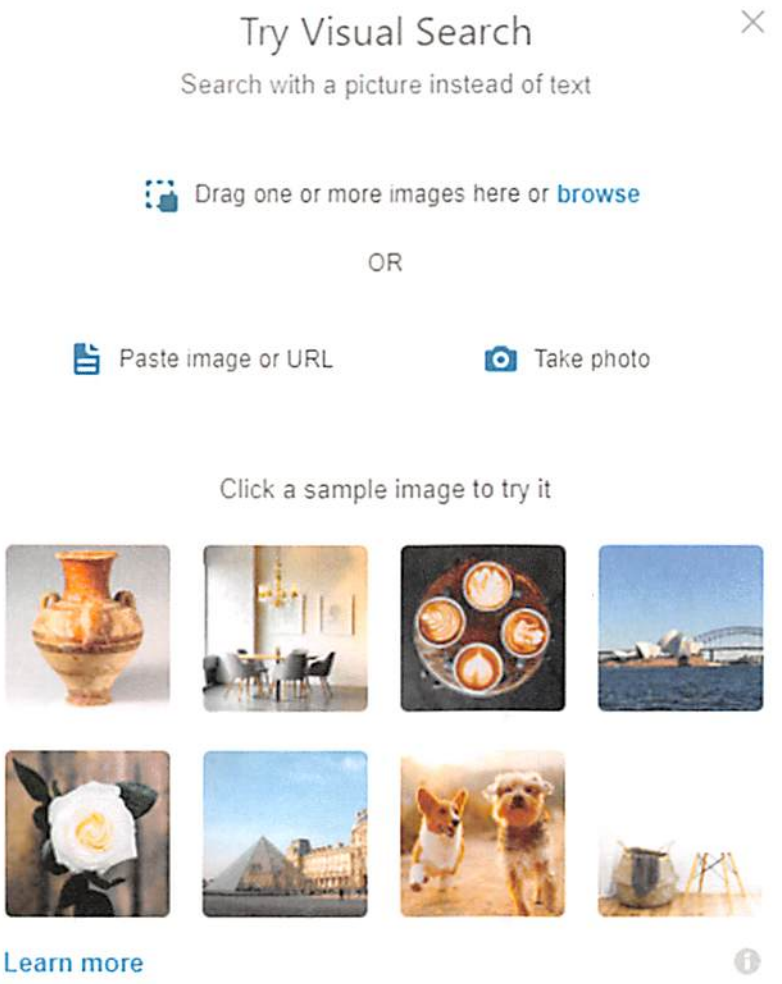
Microsoft Bing

32. Bing is a search engine owned and operated by Microsoft. Bing provides a variety of search services, including web, video, image and map search products. Once a user navigates to Bing.com, a user can enter a word or phrase into the search bar. A user may also select one of the categories on the top of the page. The categories are Images, Videos, Maps, News, MSN, Office, and Outlook.com. The Bing.com homepage also provides the option for a user to sign in to their account with Microsoft. An image of the Bing.com homepage is depicted below:

33. By selecting the "Images" tab on the Bing search engine, a user can search for images by typing in a word or phrase into the search bar, as depicted below:



34. Bing provides an option in the search bar that allows the user to search by image, which is indicated by a camera icon in the search bar. If a user hovers over the camera icon with their mouse, a box appears stating, "Search using an image." Once a user clicks on the camera icon, a box pops up stating, "Try Visual Search" and "Search with a picture instead of text". The pop up box further notes that the user can "Drag one or more images here or browse", "Paste image or URL" or "Take photo". This pop up box is depicted below:



35. By clicking on "browse", the user can select any image located on their computer to upload to BingImage. After the desired image is selected, the user chooses the "Open" button, and the image is uploaded in BingImage. Once an image is uploaded to BingImage, related images appear to the right of the uploaded image on BingImage. A user does not need a Microsoft account to upload an image to BingImage.

Probable Cause to Search the Subject Premises

36. On August 28, 2019, Microsoft BingImage filed Cybertipline Report 54255529 with the National Center for Missing and Exploited Children (NCMEC). The Cybertip states that a user at the IP address 70.104.170.54 uploaded one image containing child pornography on August 27, 2019, at 02:08:58 UTC. The Cybertip states the Electronic Service Provider (ESP) viewed the entire contents of the uploaded file. The Cybertip was initially forwarded to the Virginia State Police, Northern Virginia (NOVA) Internet Crimes Against Children (ICAC) Task Force for investigation.

37. On September 26, 2019, Special Agent Michael Bullock, Virginia State Police, served an administrative subpoena on Verizon for account information belonging to the IP address 70.104.170.54 on August 27, 2019, at 02:08 UTC. Verizon provided the account holder for the IP address was "hopkins zachary", **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608**. The IP address was assigned on March 10, 2019 through September 17, 2019. The Virginia State Police forwarded the Cybertip to the Southern Virginia (SOVA) ICAC Task Force for investigation, based on the location of the location of the residence.

38. In October 2019, Task Force Officer (TFO) Heather Call received the Cybertip from the SOVA ICAC Task Force. TFO Call reviewed the image associated with the Cybertip. The image features a nude juvenile male and a clothed juvenile female. There is an unknown aged person off to the side, who is only partially visible. The unknown aged person has their hand on the male's penis.

39. On November 15, 2019, TFO Call served a Grand Jury Subpoena on Dominion Virginia Power for account information associated with **32 Cedarwood Way, Apartment C,**

Newport News, Virginia, 23608. Dominion Virginia Power identified the customer as Zachary C. Hopkins.

40. On November 22, 2019, from 7:08-7:40 am, TFO Call conducted surveillance at **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608.** TFO Call observed a SUV parked in the parking lot bearing Virginia registration RU133T. A check with the Virginia Department of Motor Vehicles (DMV) showed this vehicle as a 2012 green Ford four door registered to Zachary Clay Hopkins, **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608.**

41. On December 6, 2019, from 7:20-8:00 am, TFO Call conducted surveillance at **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608.** TFO Call observed a SUV parked in the parking lot bearing Virginia registration RU133T. A check with the Virginia Department of Motor Vehicles (DMV) showed this vehicle as a 2012 green Ford four door registered to Zachary Clay Hopkins, **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608.**

42. Your affiant checked the Clear information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) and did not locate anyone else associated with **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608.**

Conclusion

43. Based on the facts set forth above, your affiant believes probable cause exists that located at **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608,** are violations of Title 18, United States Code, § 2252A(a)(2) and (a)(5)(B), which prohibits the knowing receipt

or distribution of child pornography (and any visual depictions of and involving the use of a minor engaging in sexually explicit conduct) in interstate or foreign commerce, and the knowing possession of one or more matters containing an image of child pornography (and any visual depictions of and involving the use of a minor engaging in sexually explicit conduct) that have traveled in interstate or foreign commerce or were produced using material so transported or shipped.

44. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities (more precisely described in Attachment B) of such violations will be found at the premises of **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608** (more precisely described in Attachment A.)

45. Accordingly, your affiant requests that a search warrant be issued authorizing FBI agents, representatives of the FBI, with assistance from representatives of other law enforcement agencies as required, to search **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608,** (more precisely described in Attachment A), for evidence, fruits, and instrumentalities (more precisely described in Attachment B) of the offenses described in paragraph 8 and 9 of this affidavit.

46. It is further requested that this affidavit, search warrant, and the subsequent inventories be sealed in order to protect the confidentiality of the sources of information and the ongoing investigation.

FURTHER AFFIANT SAYETH NOT.

Heather Call
Special Deputy United States Marshal
FBI Child Exploitation Task Force
Federal Bureau of Investigation

This affidavit has been reviewed for legal sufficiency by Assistant United States Attorney Lisa R. McKeel.

Reviewed:
Lisa R. McKeel
Assistant United States Attorney

Subscribed and sworn before me this 9th day of January, 2020, in the City of Newport News, Virginia.

UNITED STATES MAGISTRATE JUDGE

Douglas E. Miller
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched is the residence and all outbuildings contained thereupon the property as follows:

The residence is located at **32 Cedarwood Way, Apartment C, Newport News, Virginia, 23608.** It is described as an apartment building with tan siding and white trim. The number "32" is posted on the side of the building. The letter "C" is posted to the left of the apartment door, which is on the first floor.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

The items to be seized as evidence, fruits, and instrumentalities of the violation of Title 18, United States Code (U.S.C.), Sections 2252A(a)(2) and (a)(5)(B), include the following:

1. Records, documents, materials, videos, and photographs, pertaining in any way to child pornography and visual depictions of minors engaged in sexually explicit conduct (hereinafter collectively referred to as "child pornography"), child erotica, and materials pertaining to an interest in child pornography, in whatever format found.

2. Records, documents, materials, and correspondence pertaining to the possession, receipt or distribution of child pornography, and any records indicating whether such was transmitted or received using a computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail.

3. Records, documents, materials, envelopes, letters, and other correspondence including electronic mail, chat logs, and electronic messages, seeking to obtain and/or offering to transmit child pornography through interstate or foreign commerce, including U.S. mail or by computer.

4. Records, documents, materials, envelopes, letters, and other correspondence including electronic mail, chat logs, and electronic messages, identifying persons transmitting or offering to transmit any visual depictions of minors engaged in sexually explicit conduct and any records identifying the means of such transmission.

5. Records, documents, materials, and photographs depicting sexual conduct, whether between adults and minors or between minors.

6. Records, documents, materials evidencing occupancy or ownership of the premises to be searched, including but not limited to, utility bills, mail envelopes, or addressed correspondence.

7. Records, documents, materials or other items which evidence ownership or use of computer and electronic equipment found in the above residence, including sales receipts, bills for Internet access, records containing account/user names and passwords, handwritten notes, and handwritten notes in computer manuals.

8. Records, documents, and materials pertaining to the production, reproduction, receipt, shipment, ordering, soliciting, trading, purchasing, or transactions of any kind involving the transmission through interstate or foreign commerce, including by U.S. mail or other common carrier or by computer or electronic device, of child pornography.

9. Records, documents, and materials, including bank, financial, and credit card records, pertaining to the purchase of materials or access to materials containing child pornography.

10. Computer hardware, including central processing units (CPUs), computer software and programs, laptop computers, monitors, keyboards, printers, computer disks (including floppy disks, CDs, DVDs), scanners, disk drives, modems, routers, magnetic storage media, thumb or flash drives, memory sticks, PDAs, digital cameras and memory cards, cell phones, smartphones, I-Phones, I-Pods, I-Pads, electronic notebooks and tablets, hardware and software operating manuals, post-it notes, records containing account/user names and passwords, and other computer-related and/or electronic equipment and/or digital media, to be inspected off-site using appropriate mirror-imaging and other equipment after seizure, which are used as instrumentalities of the crimes noted or which contain any of the items noted in paragraphs 1-9 above.

11. Any of the items described in paragraphs 1-9 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment, including floppy diskettes, fixed hard drives, removable hard drives, software, PDAs, cell phones, or memory in any form, to be inspected off-site using appropriate mirror-imaging and other equipment after seizure.